Wireless Networks Technologies and Applications

Presented by Jorge Palau
U.S. Army Information Systems Engineering Command
Fort Huachuca, Arizona

June 23rd, 2004

OUTLINE

- Overview of Wireless Technologies
  - Wireless Local Area Networks (IEEE 802.11)
  - Wireless Metropolitan Area Networks (IEEE 802.16)
  - Other (Free Space Optics, Millimeter Wave)
- Applications, Strengths, Vulnerabilities
- Policy and Guidance
- Security Certification and Accreditation

Overview of Wireless Technologies

- IEEE 802.11 Family of Standards for Wireless Local Area Networks
  - 802.11: 2.4 GHz, 1 & 2 Mbps
  - 802.11a: 5 GHz, 54 Mbps
  - 802.11b: 2.4 GHz, 11 Mbps
  - 802.11g: 2.4 GHz, 54 Mbps
- Wi-Fi Alliance
  - Industry non-profit organization promotes adoption and use of 802.11 standard technologies, interoperability and conformance testing
  - Wi-Fi certification
- IEEE 802.11 Range
  - 60 to 300 Feet indoors
  - Up to 1000 Feet outdoors
  - We achieved 67 miles with high gain directional antennas
  - Data throughput decreases as distance to access point increases

Overview of Wireless Technologies- I

- IEEE 802.11 Issues:
  - Interference in the 2.4 GHz band
  - Scalability of 802.11b (the most popular and commonly used) supports up to 3 non-overlapping channels
  - 802.11a supports up to 12 non-overlapping channels but at reduced ranges (~ 5x less than 802.11b) with fast performance drop-off
  - Security is by far the most significant issue for military users:
    - An access point is a door into your network (effective and easy to use hacking tools freely available)
    - Mind-boggling number of ways to compromise an access point: Wired Equivalent Privacy (WEP) compromise, ARP cache poisoning, access point spoofing, credential compromise, to name a few – imagination is the limit; very hard to detect
    - Wi-Fi Protected Access (WPA), the interim security enhancement by the Wi-Fi alliance is better but not suitable either
    - Access point transmissions have been picked up as far as 15-20 miles away

"THERE IS NO SECURITY, ONLY ETERNAL VIGILANCE"

Overview of Wireless Technologies- II

- Future 802.11 Standards Enhancements
  - 802.11e: MAC layer enhancements for QoS (interesting to see it work with packet error rates that can be as high as 20%); expected no earlier than 2005
  - 802.11n: Minimize protocol overhead, increase data rates (100 Mbps or more), greater capacity, multiple input / multiple output; expected in 2006
  - 802.11s: Mesh networking; expected 2006
  - 802.11i: Update to 802.11 security that includes all of the WPA, and also adds stronger encryption using AES and quick handoff through re-authentication among access points. AES has higher computational requirements, and some devices may need replacement; standard ratification expected this summer

Overview of Wireless Technologies - I

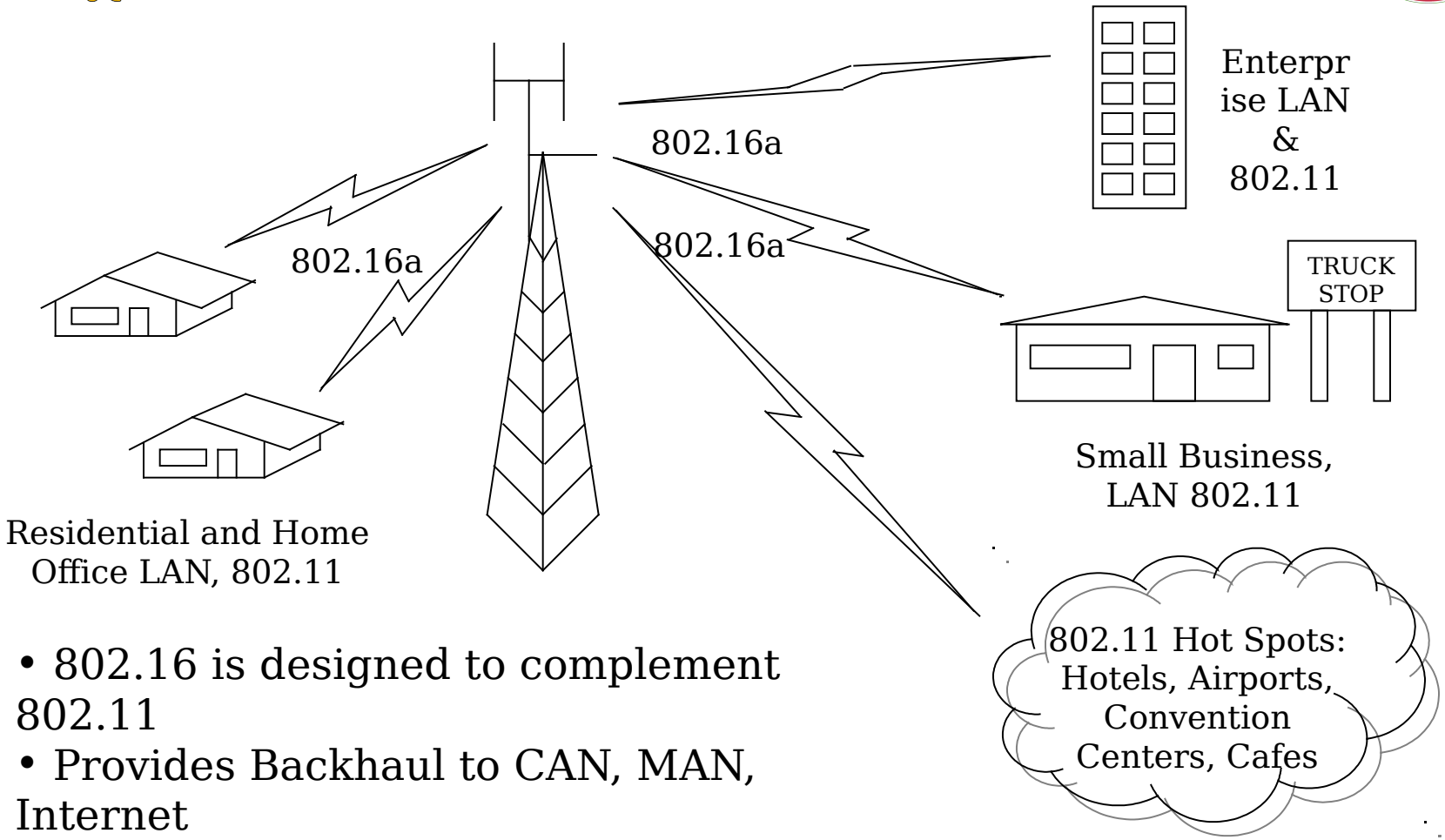
- IEEE 802.16 Family of Standards for Metropolitan Area Networks
  - 802.16: 10 - 66 GHz, 134 Mbps (28 MHz), LOS
  - 802.16a: 2 - 11 GHz, 70 Mbps (14 MHz), Licensed & Exempt, Non LOS
  - 802.16c: 10 – 66 GHz, Detailed system profiles
  - 802.16d: 2-11 GHz, ongoing revision, it consolidates all of the above, retaining all modes and major features. Defines standard system profiles to which manufacturers can test compliance.
  - 802.16e: 2 – 6 GHz Licensed, ongoing enhancement to IEEE Std 802.16/802.16a in support of mobile users (vehicular speeds up to 100 MPH), laptop chipsets expected in 2006.
- Wi-MAX Alliance
  - Industry non-profit organization promotes adoption and use of 802.16 standard technologies, interoperability and conformance testing
  - Wi-MAX certification (Not Available Yet)
- IEEE 802.16 Range
  - Nominal range is 30 miles LOS and 4 miles non-LOS

Overview of Wireless Technologies - V

Other Wireless Technologies

- Free Space Optics (FSO): Point-to-point LASER beam, 2-3 km range, 1 Gbps (lower rates also available), Full Duplex
  - FSO systems are Layer 1 products (protocol independent) and typically interface with your network switch, hub, bridge or router via multimode fiber (850nm or 1310nm) and standard ST or SC connectors
  - Hawaii demonstration later this summer; preliminary results: link maintained through fog at 4,402 feet
- Millimeter Wave: Point-to-point (PTP), 57-64 GHz (or higher for some products), 8-10 mile maximum range, 100 Mbps to 1 Gbps, Full Duplex
  - Layer 1 and protocol independent (same as above)
  - Availability suffers at maximum range

Applications, Strengths, Weaknesses



- 802.16 is designed to complement 802.11
- Provides Backhaul to CAN, MAN, Internet
- Backhaul can also be achieved using point-to- point FSO or millimeter wave

pplications, Strengths, Weaknesses -

- 802.11
  - Strengths: Ubiquitous and convenient user access, easy deployment, low cost
  - Weaknesses: Bandwidth contention (Carrier Sense Multiple Access (CSMA)), no QoS, half duplex, shares 2.4 GHz with commercial products (cordless phones, microwave ovens), very vulnerable potential “back door”
- 802.16
  - Strengths: Multiple services with full QoS, can be Full Duplex (grant/request mechanism rather than CSMA), Non LOS, Point-to-point & Point-to-multipoint (PTP & PMP)
  - Weaknesses: Interference, still emerging
- Free Space Optics
  - Strengths: High bandwidth, no RF interference, narrow beam
  - Weaknesses: Susceptible to fog at long distances, Unknown O&M
- Millimeter Wave
  - Strengths: High bandwidth; narrow beam, O2 absorption at 60 GHz
  - Weaknesses: RF interference, rain

pplications, Strengths, Weaknesses - L

- Wireless is simply not as reliable as wire and fiber. The strength of wireless lies in providing convenient network access (802.11), and Internet/WAN connectivity without incurring buried cable costs (802.16, FSO, etc).
- 802.11 is best for typical network use (unicast web, e-mail, file transfer) at short range and without high availability. Not designed for backbone/backhaul but it is being done. Ideal applications include:
  - In warehouses, private homes
  - As a backup or in conjunction with wired LANs
  - In public areas at airports, hotels, meeting places, truck stops, libraries, etc
- 802.16 is best if guaranteed bandwidth and low delays are necessary. More robust and better suited for backhaul and network backbone applications than 802.11. Availability can be a problem due to interference.
- FSO appears very promising for backhaul applications at medium distances (1 Gbps at 2-3 kilometers, newer models offer greater bandwidth)
- Point-to-point millimeter wave is also a viable option depending on the requirements
- Wireless backhaul technologies can have low bandwidth back up if copper is available

Policy and Guidance Documents

- National Security Telecommunications and Information Systems Security Policy (NTISSP) #11 (National Information Assurance Acquisition Policy):
  All COTS IA and IA enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting national security information) must be evaluated and validated according to the NIAP / Common Criteria or NIST FIPS testing and evaluation schemes, effective July 2002 (Crypto not covered in NIAP/CC)
- DoDD 8500.1 and DoDI 8500.2: Mandate compliance and provide guidance for NSTISSP #11
- Defense Information Systems Agency (DISA) Wireless Security Technical Implementation Guide (STIG) Published tool to assist improvement of security in wireless systems, used in conjunction with the Network & OS appropriate STIGS (Version 1 Release 4, 10 July 2003 and Version 3 Release 0 (Draft) 15 March 2004 -adds WPAN – 802.15 & RSN – 802.11i)
- U.S. Army Regulation (AR) 25-2, Information Assurance, 14 November 2003
- DISA Wireless Security Support Program (Wireless LAN Security Framework January 2004)
- Department of Defense (DoD) Directive 8100.2: Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid (GiG) 14April 2004
- U.S. Army, Network Enterprise Command (NETCOM): Wireless Best Business Practices (BBPs), To Be Released Soon

olicy and Guidance Requirements (Highlight

- Wireless links passing unclassified data must be encrypted end-to-end (at layer 2) using FIPS 140-2 certified products (3DES or AES are the only acceptable algorithms)
- 802.11 Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) security are not acceptable for FIPS 140-2 certification, or for use in conjunction with Layer 3 encryption in lieu of a certified solution
- 802.11 cannot be used for Top Secret data
- 802.11 solutions require wireless intrusion detection and firewalls
- 802.11 solution should be able to detect and suppress rogue access points
- 802.11 solution should incorporate a location aware protection scheme (security policies are enforced based on location of access points and users)
- Personal firewalls are only mandated for traveler's laptops, however they should also be used in wireless LAN capable computers
- Type 1 encryption is mandated for Secret data (Harris SecNet-11 is the only NSA-approved solution)
- In the future FIPS 140-2 Level 2 certification will be required

Security Certification & Accreditation

"Security certification is the comprehensive evaluation of the technical and non technical security features of an AIS and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements." AR 380-19, Chapter 5

- Certification testing is undertaken to obtain an impartial statement on the ability of a given system to satisfy it's security requirements, and as a basis to determine the resultant risk .
- Certification Testing includes:
  - Automated and Manual Vulnerability Scans and Assessments
  - Physical and Personnel Security Procedures
  - Interviews of system personnel
  - Plans for security sustainment, etc
- Based on the results, the certifier will make a recommendation to the DAA (the certifier is not the decision maker.)
- Director of IASED, USAISEC, is the Certification Authority for most PEO EIS Systems

ecurity Certification & Accreditation-

- Security accreditation, according to AR 25-2, is defined as

  “the official management authorization to operate an IS or network and is based, in part, on the formal certification of the degree to which a system meets a prescribed set of security requirements. The C&A statement affixes security responsibility with the accrediting authority.”

- Accreditation must address each operational environment of the IS for both fixed and deployable configurations.
- DAA must decide if the security of the system is good enough and the risks can be assumed

ecurity Certification & Accreditation - II

- Important points on Information Assurance
  - Information Assurance is not a discrete event
  - Information Assurance is achieved only after a thoughtful, holistic systems approach has been applied to securing the entire system
  - Information Assurance is maintained only when the total system lifecycle is considered and appropriate policies, safeguards, resources and management interest is maintained
  - A secure system requires sound system engineering, security engineering, certification testing and lifecycle IA support.
  - DITSCAP is C&A focused, not security engineering.
  - Secure systems can only be sustained by a secure organization
  - We highly recommend not to take security into your own hands: make sure you consult with a security professional.

POINTS OF CONTACT

- USAISEC, Technology Integration Center
  Mr. Dan Bradford, Director
  BradfordD@hqisec.army.mil
  520.533.7195, DSN 821.7195

- USAISEC, Information Assurance & Security Engineering Directorate
  Mr. Ted Hendy, Director
  HendyT@hqisec.army.mil
  520.538.7003, DSN 879.7003

- Slide Content: Jorge Palau, Palauj@hqisec.army.mil, 520.533.3921 DSN 821